

Set IBE encryption in FortiMail 5.2.x from scratch.

1. Go to Encryption -> IBE

You can use all the default settings here, only enable the IBE service, and set the base URL or IP address starting with HTTPS. Click “Apply” when finished.

The screenshot shows the FortiMail VM web interface with the 'IBE Encryption' tab selected. The 'Enable IBE service' checkbox is checked. The 'IBE service name' is set to 'Encryption'. The 'User registration expiry time (days)' is 30, 'User inactivity expiry time (days)' is 90, and 'Encrypted email storage expiry time (days)' is 180. The 'Password reset expiry time (hours)' is 24. The 'Allow secure replying' checkbox is checked. The 'Allow secure forwarding' and 'Allow secure composing' checkboxes are unchecked. The 'IBE base URL' is set to 'https://172.31.16.63'. The 'Notification Settings' section is expanded, showing options for sending notifications when a message is read, if it remains unread for 14 days, to the sender, and to the recipient. The 'Apply' button is at the bottom.

2. Go To Profile -> Content

Click the “New...” button to create a profile

The screenshot shows the FortiMail VM web interface with the 'Content' tab selected. The 'New...' button is highlighted. Below the button is a table of existing content profiles:

Profile Name	Domain Name
CF_Inbound	System
CF_Outbound	System
content_basic_predefined	System
content_out_basic_predefined	System
content_sofilter	System

3. Set the domain to “--System--”, type a name for the new profile and set the direction.

Click the “New...” button next to the “Action:” box to create new Action Profile

The screenshot shows the FortiMail VM web interface with the 'Content Profile' configuration page. The 'Domain' is set to '--System--', the 'Profile name' is 'Encrypt_IBE', and the 'Direction' is 'Outgoing'. The 'Action' is set to '--None--', and the 'New...' button next to it is highlighted. Below the configuration fields are sections for 'Attachment Filtering', 'File Type Filtering', 'Other Setting', 'Scan Conditions', and 'Content Monitor and Filtering'. The 'Create' and 'Cancel' buttons are at the bottom.

4. Enable the option “Encrypt with profile:”, select encryption profile from the list or click “New...”:

FortiMail Content Action Profile

Domain: --System--

Profile name:

Direction: Outgoing

☐ Tag email's subject line With value:

☐ Insert new header With value:

☐ Deliver to alternate host

☐ BCC

☐ Archive to account --None-- New... Edit...

☐ Notify with profile --None-- New... Edit...

☐ Treat as spam

☐ Reject

☐ Discard

☐ Replace

☐ Personal quarantine

☐ System quarantine

☐ Rewrite recipient email address

☒ Encrypt with profile --None-- New... Edit...

Create Cancel

5. Set the the new profile and click “Create”. For example:

FortiMail Encryption Profile

Profile name: IBE_Push

Protocol: IBE

Access method: Push

Maximum size (KB) for Push method: 1024

Encryption algorithm: Triple DES

Action: Encrypt

Action on failure: Drop and send DSN

Create Cancel

6. Check the settings in the “Content Action Profile”, select a profile name, and click “Create”

FortiMail Content Action Profile

Domain: --System--

Profile name: Action_Encrypt_IBE

Direction: Outgoing

☐ Tag email's subject line With value:

☐ Insert new header With value:

☐ Deliver to alternate host

☐ BCC

☐ Archive to account --None-- New... Edit...

☐ Notify with profile --None-- New... Edit...

☐ Treat as spam

☐ Reject

☐ Discard

☐ Replace

☐ Personal quarantine

☐ System quarantine

☐ Rewrite recipient email address

☒ Encrypt with profile IBE_Push New... Edit...

Create Cancel

7. You will return to the Content Profile.

Click the arrow next to Content Monitor and Filtering to expand the submenu and click “New...”

USER

Policy

Profile

Session

AntiSpam

AntiVirus

Content

Authentication

LDAP

Dictionary

Security

IP Pool

Group

Attachment Filtering

File Type Filtering

Other Setting

Scan Conditions

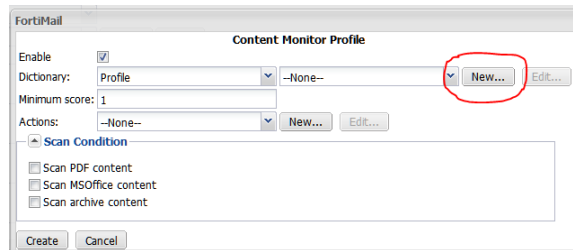
Content Monitor and Filtering

New... Edit... Move Delete

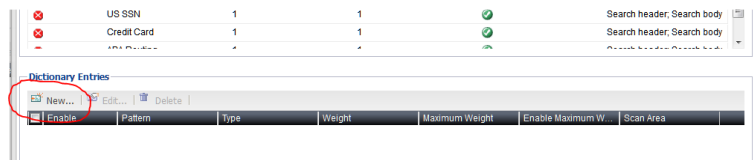
Enable Dictionary Group Dictionary Profile Minimum Score Action

8. Now you need to create a new dictionary profile

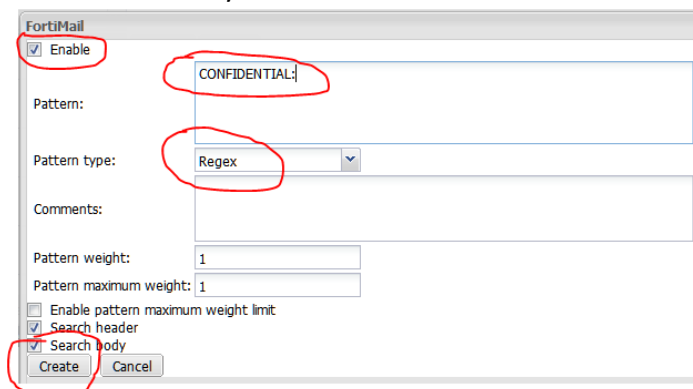
Click “New...” next to the “Dictionary:” boxes



9. Click “New...”

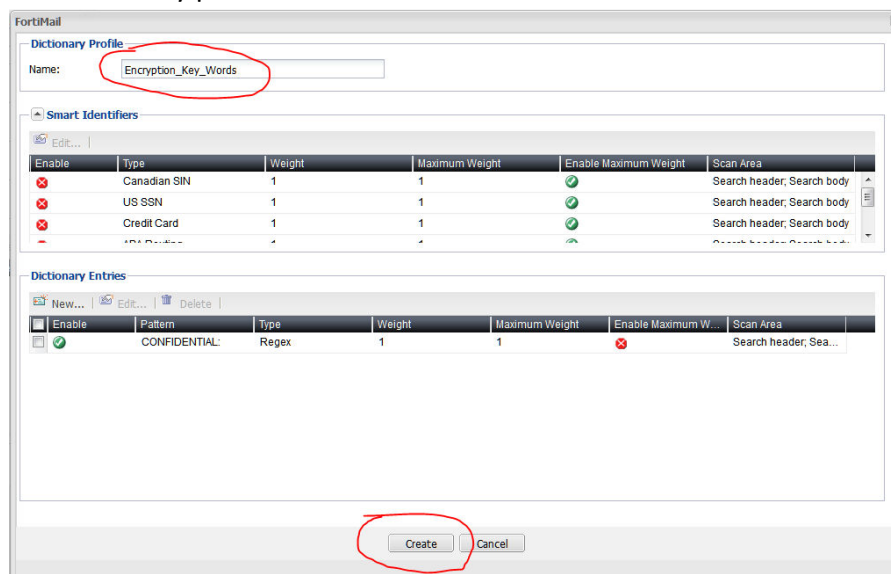


10. Type the pattern you want to use as a keyword and click “Create”



11. If you need to create more than one keyword to activate the encryption, repeat 9) and 10)

12. Select name for the dictionary profile and click “Create”



13. Select the previously created action and click “Create”

FortiMail Content Monitor Profile

Enable ☒

Dictionary: Profile Encryption_Key_Words New... Edit...

Minimum score: 1

Actions: Action_Encrypt_IBE New... Edit...

Scan Condition

☐ Scan PDF content

☐ Scan MSOffice content

☐ Scan archive content

Create Cancel

14. Now we are back to the Content Profile.
Check the settings and click “Create”

FortiMail VM

Monitor Content Action

Content Profile

Domain: triton.bg

Profile name: Profile Encrypt IBE

Direction: Incoming

Action: Action_Encrypt_IBE New... Edit...

Attachment Filtering

File Type Filtering

Other Setting

Scan Conditions

Content Monitor and Filtering

Enable	Dictionary Group	Dictionary Profile	Minimum Score	Action
<input checked="" type="checkbox"/>	-	Encryption_Key_...	1	Action_Encrypt_IBE

Create Cancel

15. The content profile was created.

FortiMail VM

Basic Mode >>

Help Wizard Log Out FORTINET

Profile Name	Domain Name	Direction
CF_Inbound	system	Incoming
CF_Outbound	system	Outgoing
Encrypt_IBE	system	Outgoing
content_basic_predefined	system	Incoming
content_out_basic_predefined	system	Outgoing
content_sotter	system	Incoming

16. Add the new Content profile to an outgoing recipient-based policy.

Note: If secured replying is used the content profile must be also added to an Incoming recipient-based policy.